Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Algebra 305 (2006) 130–145

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Normal subgroups generated by a single pure element in quaternion algebras

Louis Rowen[a,1], Yoav Segev[b,*,2]

[a] *Department of Mathematics, Bar-Ilan University, Ramat Gan, Israel*
[b] *Department of Mathematics, Ben-Gurion University, Beer-Sheva 84105, Israel*

Received 22 August 2005

Available online 13 December 2005

Communicated by Aner Shalev

Abstract

Let D be a quaternion division algebra whose center is an arbitrary infinite field K of characteristic $\neq 2$, and let $e \in D$ be a pure quaternion. Hence, by definition, $e \in D \setminus K$ and $e^2 \in K$. We show that if the characteristic of K is > 2, then $D^\times/\langle e^{D^\times}\rangle$ is abelian-by-nilpotent-by-abelian. Note that by [A.S. Rapinchuk, L. Rowen, Y. Segev, Nonabelian free subgroups in homomorphic images of valued quaternion division algebras, Proc. Amer. Math. Soc., in press] this result is false in characteristic zero. As a consequence we show that the Whitehead group $W(G,k)$, where G is an absolutely simple simply connected algebraic group of type ${}^{3,6}D_4$ defined over a field k of odd characteristic and of k-rank 1, is abelian-by-nilpotent-by-abelian.

Keywords: Quaternion division algebra; Pure quaternion; Whitehead group

* Corresponding author.
E-mail addresses: rowen@macs.biu.ac.il (L. Rowen), yoavs@math.bgu.ac.il (Y. Segev).

1 Partially support by BSF grant no. 2004-083 and by the Israel Science Foundation Center of Excellence.
2 Partially supported by BSF grant no. 2004-083.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.11.015

1. Introduction

The main goal of this paper is to restrict the structure of the Whitehead group of algebraic groups of type ${}^{3,6}D_4$ defined over an arbitrary infinite field k and of k-rank 1. Let us briefly recall the definition of the Whitehead group.

Let G be an absolutely simple algebraic group defined over k. The subgroup $G(k)^+$ of $G(k)$, is the subgroup generated by the k-rational points of the unipotent radicals of k-defined parabolic subgroups of G. The quotient $W(G,k) = G(k)/G(k)^+$ was termed the Whitehead group by J. Tits in [Ti].

The following explicit description of the Whitehead group $W(G,k)$ when G is of type ${}^{3,6}D_4$ and of k-rank 1, and when $\mathrm{char}(k) \neq 2$ was recently obtained by Gopal Prasad in [Pr]: There exists a quaternion division algebra D whose center K is a cubic separable extension of k and whose corestriction to k is trivial (see Section 3) such that if we set

$$U := \langle x \in D^\times \mid \mathrm{Nrd}(x), \mathrm{Trd}(x) \in k \rangle \quad \text{and} \quad V := \{ x \in D^\times \mid \mathrm{Nrd}(x) \in k \},$$

where Nrd and Trd are respectively the reduced norm and trace, then

$$W(G,k) \text{ is a homomorphic image of } V/U,$$

and in some cases, e.g. when k is a perfect field, $W(G,k) = V/U$. In this paper, the machinery we were able to develop in order to restrict the structure of V/U uses the fact that U contains an element $e \in D^\times \setminus K$ such that $e^2 \in k$ (see Section 3). Thus our first main result is the following.

Theorem A. *Let D be a quaternion division algebra of odd characteristic. Let $e \in D^\times$ be a noncentral element such that e^2 is in the center. Then the quotient of $D^\times$ over the normal closure of e is abelian-by-nilpotent-by-abelian.*

See Theorem 6.1 for a precise formulation of "abelian-by-nilpotent-by-abelian." We note that a better result when $\mathrm{char}(D) = 3$ is given in Corollary 6.4. Notice that Theorem A is false in characteristic zero; see [RaRoS] for a counterexample.

As an immediate corollary to Theorem A we get:

Theorem B. *Let k be an infinite field of odd characteristic and let G be an absolutely simple, simply connected algebraic group of type ${}^{3,6}D_4$, defined over k and of k-rank* 1. *Then the Whitehead group $W(G,k)$ is abelian-by-nilpotent-by-abelian.*

We mention that Section 5 contains a variety of results on normal subgroups of $D^\times$ for any quaternion division algebra D in *arbitrary characteristic*; they may become useful in further research on the structure of the Whitehead group and, more generally, on the structure of $D^\times$.

The structure of the multiplicative group $\mathcal{D}^\times$ of a finite-dimensional division algebra $\mathcal{D}$ is, by and large, rather mysterious. Of course it is known to be nonsolvable and, being a subgroup of $\mathrm{GL}_n(F)$ (for some n and F) one can apply "linear" techniques on $\mathcal{D}^\times$;

but, since $\mathcal{D}^{\times}$ contains no unipotent elements, this approach has severe limitations. New techniques for $\mathcal{D}^{\times}$ were started in [S] and further developed in [RaS,RaSSei], where it was shown that finite homorphic images of $\mathcal{D}^{\times}$ are solvable. In this paper we investigate homomorphic images which are not necessarily finite.

We conclude the introduction by mentioning that recently Gopal Prasad [Pr] proved, using very different (arithmetic) techniques that when k is a global field, and G is as in Theorem B, $W(G,k)=1$, thus proving the Kneser–Tits conjecture in this case.

2. Notation, definitions and preliminaries

Throughout this paper D denotes a quaternion division algebra and K denotes its center. Thus D is a division algebra of dimension 4 over its center. We denote by $D^{\times} := D \setminus \{0\}$ the multiplicative group of D. Now D has a basis over K of the form

$$1, e, f, ef, \quad e^2 = a \in K^{\times}, \quad f^2 = b \in K^{\times}, \quad ef = -fe, \quad \text{if } \operatorname{char}(K) \neq 2, \tag{2.1}$$

$$1, e, f, ef, \quad e^2 + e = a \in K^{\times}, \quad f^2 = b \in K^{\times}, \quad ef = f(e+1), \quad \text{if } \operatorname{char}(K) = 2. \tag{2.1$'$}$$

Each element $x \in D$ can be written uniquely in the form

$$x = \alpha + \beta e + \gamma f + \delta ef, \quad \alpha, \beta, \gamma, \delta \in K, \tag{2.2}$$

or

$$x = \mu + \eta f, \quad \mu, \eta \in K(e), \tag{2.3}$$

where $K(e) = \{\alpha + \beta e \mid \alpha, \beta \in K\}$ is the (commutative) subfield of D generated by K and e, $\mu = \alpha + \beta e$ and $\eta = \gamma + \delta e$.

The map

$$\bar{\ }: \alpha + \beta e + \gamma f + \delta ef \to \alpha - \beta e - \gamma f - \delta ef, \quad \text{if } \operatorname{char}(K) \neq 2, \tag{2.4}$$

$$\bar{\ }: \alpha + \beta e + \gamma f + \delta ef \to (\alpha + \beta) + \beta e + \gamma f + \delta ef, \quad \text{if } \operatorname{char}(K) = 2 \tag{2.4$'$}$$

is called the *standard involution* of D. For an element $x \in D$ we denote by $\bar{x}$ its image under the standard involution. The standard involution is an anti-automorphism of D, that is, $\overline{x+y} = \bar{x} + \bar{y}$, $\overline{\alpha x} = \alpha \bar{x}$, $\overline{xy} = \bar{y}\bar{x}$ and $\bar{\bar{x}} = x$, for all $x, y \in D$, and $\alpha \in K$.

D has many bases as in equations (2.1) or (2.1$'$), and we make the following definitions.

Definitions 2.1.

(1) Any basis of D as in Eq. (2.1) or Eq. (2.1$'$) will be called a *standard basis* of D.
(2) When $\operatorname{char}(K) \neq 2$, an element $e \in D \setminus K$ such that $e^2 \in K$ will be called a *pure quaternion*. We denote by $\operatorname{Pure}(D)$ the set of all pure quaternions of D. (We mention that in characteristic 2 it seems more natural, in our context, to call elements $e \in D \setminus K$ pure if $e(e+1) \in K$, but we will not pursue this point further in this paper.)

(3) Suppose $\operatorname{char}(K) \neq 2$ and let $e \in \operatorname{Pure}(D)$. If an element $f \in D$ satisfies $ef = -fe$, we will say that f *anti-commutes* with e.
(4) Given a standard basis $\{1, e, f, ef\}$ of D as in (2.1) or (2.1′) and an element $x = \alpha + \beta e + \gamma f + \delta ef \in D$, the (reduced) *norm* of x is denoted in this paper by $\mathfrak{N}(x)$ and defined by $\mathfrak{N}(x) = x\bar{x}$, so

$$\mathfrak{N}(x) = \begin{cases} \alpha^2 - \beta^2 a - \gamma^2 b + \delta^2 ab & \text{if } \operatorname{char}(K) \neq 2; \\ \alpha(\alpha + \beta) + \beta^2 a + \gamma(\gamma + \delta)b + \delta^2 ab & \text{if } \operatorname{char}(K) = 2. \end{cases}$$

(5) Notation as in (4), the (reduced) *trace* of x is denoted in this paper by $\mathfrak{T}(x)$ and defined by $\mathfrak{T}(x) = x + \bar{x}$, so

$$\mathfrak{T}(x) = \begin{cases} 2\alpha & \text{if } \operatorname{char}(K) \neq 2; \\ \beta & \text{if } \operatorname{char}(K) = 2. \end{cases}$$

Note that for $\operatorname{char}(K) \neq 2$, an element $x \in D^\times$ is a pure quaternion iff $\mathfrak{T}(x) = 0$, furthermore any maximal subfield of D contains pure quaternions.

Any element $x \in D \setminus K$, has a quadratic minimal polynomial over K,

$$m_x[\lambda] = \lambda^2 - \mathfrak{T}(x)\lambda + \mathfrak{N}(x) \in K[\lambda], \tag{2.5}$$

this shows that the trace and the norm of an element are independent of the choice of a standard basis. The norm

$$\mathfrak{N} : D^\times \to K^\times,$$

is a group homomorphism. Note that if $x \in D$ is given as in equation (2.3), then

$$\mathfrak{N}(x) = \mathfrak{N}(\mu) - \mathfrak{N}(\eta)b, \quad \text{where } x = \mu + \eta f,\ \mu, \eta \in K(e),\ f^2 = b. \tag{2.6}$$

The trace map

$$\mathfrak{T} : D \to K,$$

is a linear functional whose kernel when $\operatorname{char}(K) \neq 2$ is $\operatorname{Pure}(D) \cup \{0\}$.

Lemma 2.2. *Assume that* $\operatorname{char}(K) \neq 2$ *and let* $e \in \operatorname{Pure}(D)$. *Then*

(1) *any element* $f \in D$ *that anti-commutes with* e *is a pure quaternion*;
(2) *there exists* $f \in D$ *that anti-commutes with* e;
(3) *if* $f \in D$ *anti-commutes with* e, *then the set of elements that anti-commute with* e *is precisely the set* $\{\rho f \mid \rho \in K(e) \setminus \{0\}\}$.

Proof. These are well-known facts. We briefly mention that (1) follows from the fact that f^2 commutes with both f and e so $f^2 \in K$. For (2) note that any nonzero element of the form $ex - xe$ is pure and anti-commutes with e, and (3) is easily verified. □

Lemma 2.3. *Assume that* $\operatorname{char}(K) \neq 2$ *and let* $e \in \operatorname{Pure}(D)$ *and* $f \in D$ *with* $ef = -fe$. *Then any element* $E \in \operatorname{Pure}(D)$ *has the form*

$$E = \beta e + \rho f, \quad \beta \in K,\ \rho \in K(e), \quad \text{and} \quad E \neq 0.$$

Proof. This is clear from Eq. (2.2) and from the fact that $\mathfrak{T}(E) = 0$. $\square$

Definitions and notation 2.4. Let R be any finite-dimensional division algebra and let F be its center. Then R has a reduced norm map $\mathfrak{N}: R^\times \to F^\times$ and we have:

(1) The degree of R, $\deg(R)$, is the square root of the dimension $\dim_F(R)$. It is a positive integer.
(2) A maximal subfield of R is a commutative subfield $P \subseteq R$, such that $F \subseteq P$ and $[P : F] = \deg(R)$.
(3) We let $\mathrm{SL}_1(R) = \{x \in R^\times \mid \mathfrak{N}(x) = 1\}$ and for a maximal subfield $P \subseteq R$, $\mathrm{SL}_1(P/F) = \mathrm{SL}_1(P) = \{x \in P^\times \mid \mathfrak{N}(x) = 1\}$.

Lemma 2.5. *Let* L/K *be a quadratic field extension with* $\operatorname{char}(K) \neq 2$, *and let* $x \mapsto \bar{x}$ *be the unique automorphism of* L *over* K. *Let* $\mathfrak{N} = \mathfrak{N}_{L/K}$ *be the norm map* $\mathfrak{N}: x \mapsto x\bar{x}$. *If* $u \in L^\times$ *has norm* 1, *then there exists* $y \in L$ *such that* $u = y\bar{y}^{-1}$.

Proof. This is of course a special case of Hilberts' theorem 90. We include the proof of this case for completeness. Let $e \in L \setminus K$ with $a := e^2 \in K$. Write $u = r + se$ $(r, s \in K)$. We solve the equation $u\bar{y} = y$. Let $y = \frac{sa}{r-1} + e$ (note that we may assume that $r \neq 1$). Then $\bar{y} = \frac{sa}{r-1} - e$ and $y/\bar{y} = r + se$ iff $y = \bar{y}(r + se)$, iff $\frac{sa}{r-1} + e = (\frac{sa}{r-1} - e)(r + se)$, iff $\frac{sa}{r-1} + e = \frac{sar}{r-1} - sa + (\frac{s^2a}{r-1} - r)e$. Of course $\frac{sar}{r-1} - sa = \frac{sa}{r-1}$ and since $\mathfrak{N}(u) = r^2 - s^2a = 1$, $\frac{s^2a}{r-1} - r = 1$. $\square$

Lemma 2.6. *Assume that* $\operatorname{char}(D) \neq 2$ *and let* $e \in \operatorname{Pure}(D)$, *then*

(1) *any element* $\neq -1$ *in* $\mathrm{SL}_1(K(e))$ *has the form* $\frac{1-\alpha e}{1+\alpha e}$, *for some* $\alpha \in K$;
(2) *any element* $\neq -1$ *in* $\mathrm{SL}_1(K(e))$ *has the form* $\frac{e-\alpha}{e+\alpha}$, *for some* $\alpha \in K$;
(3) $\mathrm{SL}_1(K(e)) = \{-u \mid u \in \mathrm{SL}_1(K(e))\}$.

Proof. (1) and (2) are immediate from Lemma 2.5, and (3) is obvious. $\square$

Lemma 2.7. *Let* $w \in \mathrm{SL}_1(D)$. *Then* $(1 + w)^2 = (\mathfrak{T}(w) + 2)w$.

Proof. Since $\mathfrak{N}(w) = 1$, we have $w^2 - \mathfrak{T}(w)w + 1 = 0$, so $w^2 + 1 = \mathfrak{T}(w)w$, and hence $(1 + w)^2 = 1 + w^2 + 2w = \mathfrak{T}(w)w + 2w = (\mathfrak{T}(w) + 2)w$. $\square$

Notation 2.8 *(Notation for groups).* Let G be a group. $H \leqslant G$ denotes that H is a subgroup of G and $H \lhd G$ denotes that H is a normal subgroup of G. Given an element $x \in G$, $\langle x^G \rangle$ denotes the normal subgroup of G generated by x. For $x, y \in G$, $x^y = y^{-1}xy$ and $[x, y] =$

$x^{-1}y^{-1}xy$; also $[x_1, x_2, \dots, x_n] = [[x_1, \dots, x_{n-1}], x_n]$. For subgroups $H_1, H_2, \dots, H_k \leqslant G$, $[H_1, H_2] = \langle [x, y] \mid x \in H_1$ and $y \in H_2 \rangle$, and $[H_1, \dots, H_k] = [[H_1, \dots, H_{k-1}], H_k]$. $\Gamma_i(G) = [G, G, \dots, G]$ ($(i+1)$-times) denotes the ith term in the lower central series of G. Of course G is nilpotent of class c if $\Gamma_{c-1}(G) \neq 1$ and $\Gamma_c(G) = 1$.

Theorem 2.9. ([L], see also [Rob, 12.3.6, p. 358].) *Let G be a group. Then the following two conditions are equivalent, and each implies that G is nilpotent of class $\leqslant 3$,*

(1) $[x, y, y] = 1$, *for all $x, y \in G$.*
(2) $\langle x^G \rangle$ *is abelian for all $x \in G$.*

Lemma 2.10. *Assume that* $\operatorname{char}(K) \neq 2$ *and let $e \in \operatorname{Pure}(D)$. Then*

$$\langle e^{D^\times} \rangle = \langle e \rangle \langle \mathrm{SL}_1(K(p)) \mid p \in \operatorname{Pure}(D) \text{ and } p \text{ anti-commutes with } e \rangle.$$

Proof. Let $A := \langle e^{D^\times} \rangle$ and $B := \langle e \rangle \langle \mathrm{SL}_1(K(p)) \mid p$ anti-commutes with $e\rangle$. To show that $A \subseteq B$ we show that $e^g \in B$, for all $g \in D^\times$. Let $f \in \operatorname{Pure}(D)$, with $fe = -ef$. Let $g \in D^\times$, then $g = \mu + \eta f$, $\mu, \eta \in K(e)$. Since $e^{\eta f} = -e$, we assume that $\mu \neq 0$. As $e^\mu = e$ (and $g = \mu(1 + \mu^{-1}\eta f)$), we may assume that $\mu = 1$, so $g = 1 + \eta f$. Then $e^{-1}g^{-1}eg = (1/\mathfrak{N}(g))e^{-1}\bar{g}eg = (1/\mathfrak{N}(g))g^2 \in \mathrm{SL}_1(K(\eta f))$ (recall that $\bar{g} = 1 - \eta f$, so $\bar{g}^e = (1 - \eta f)^e = 1 + \eta f = g$). Thus $g^{-1}eg \in e\mathrm{SL}_1(K(\eta f))$. Since ηf anti-commutes with e, the inclusion $A \subseteq B$ follows.

To show the inclusion $B \subseteq A$, let $p \in \operatorname{Pure}(D)$ such that p anti-commutes with e, and let $u \in \mathrm{SL}_1(K(p))$. Then, by Lemma 2.5, $u = \bar{g}/g$, for some $g \in K(p)$. But $g^e = \bar{g}$, so $u = \bar{g}/g = e^{-1}geg^{-1}$, and we see that $u \in A$. This shows the inclusion $B \subseteq A$ and completes the proof of the lemma. □

Lemma 2.11. (See [RaPo, Lemma 3.1] and [PRa, Lemma 4].) *Let $u \in \mathrm{SL}_1(D)$. Then*

(1) *given any maximal subfield P of D, there exist $x \in P^\times$ and $g \in D^\times$ such that $u = [x, g] = x^{-1}g^{-1}xg$;*
(2) *if $k \subseteq K$ is a subfield with $[K : k] = 3$ and $W \subseteq D$ is a k-subspace of D of dimension $\geqslant 4$, then there exist $x \in W \setminus \{0\}$ and $g \in D^\times$ such that $u = [x, g]$.*

Proof. Fix $u \in \mathrm{SL}_1(D)$ and consider the linear map $\varphi : P \to K$ defined by $\varphi(x) = \mathfrak{T}(xu) - \mathfrak{T}(x)$. Let $x \in \ker\varphi$, $x \neq 0$. Then $\mathfrak{T}(x) = \mathfrak{T}(xu)$, and of course $\mathfrak{N}(x) = \mathfrak{N}(xu)$, so, by the Skolem–Noether theorem, there exists $g \in D^\times$, such that $x^g = xu$, or $[x, g] = u$. The proof of (2) is the same as the proof of (1). □

Lemma 2.12. *Assume that* $\operatorname{char}(K) \neq 2$. *Then*

(1) *for each element $x \in D^\times \setminus \operatorname{Pure}(D)$, there exists $w \in \mathrm{SL}_1(D)$ and $\alpha \in K^\times$ such that $x = \alpha(w + 1)$;*
(2) $D^\times = K^\times \langle (w + 1) \mid w \in \mathrm{SL}_1(D) \rangle$.

Proof. (1) We may assume that $x \notin K$. Then $x = \frac{1}{\beta+e}$, for some $e \in \mathrm{Pure}(D)$ and $\beta \in K^{\times}$, so $x = \frac{1}{2\beta} \cdot (\frac{\beta-e}{\beta+e} + 1)$, and take $\alpha = \frac{1}{2\beta}$, $w = \frac{\beta-e}{\beta+e}$.

(2) Let $R = K^{\times}\langle (w+1) \mid w \in \mathrm{SL}_1(D)\rangle$ and let $y \in D^{\times}$. If y is not pure, then by (1), $y \in R$, so assume $y \in \mathrm{Pure}(D)$. Then $y+1$ and $y^{-1}+1$ are not pure, so $y+1 \in R$ and $y^{-1}(y+1) = y^{-1}+1 \in R$, hence also $y \in R$. $\square$

3. Corestriction

In this paper we are interested in the structure of V/U, where V and U are as in the introduction. The purpose of this section and the next Section 4 is to show the following. Section 4 shows that if U contains a k-subspace of a large enough dimension, then we can get information on U; however this section shows that these techniques are *not* applicable to our current situation (but they may be useful in other circumstances). We do this in a more general context. Other than reading about the corestriction in the next paragraph, the reader can skip Sections 3 and 4. *Throughout this section we assume that* $\mathrm{char}(K) \neq 2$.

Suppose K/k is a separable cubic extension. We will use [KMRT, 43.9] which states that the corestriction of D along K/k is trivial if and only if D possesses a standard basis $\{1, e, f, ef\}$ such that $e^2 \in k$ and $\mathrm{Norm}_{K/k}(f^2) = 1$.

We also note the following fact. If we denote by: $\mathrm{cor} = \mathrm{cor}_{K/k}$ (respectively $\mathrm{res} = \mathrm{res}_{K/k}$) the corestriction (respectively restriction) map, then $\mathrm{cor} \circ \mathrm{res}$ is multiplication in the Brauer group by $[K:k] = 3$, which, for a quaternion division algebra, is the same as multiplication by 1 (the order of $[D]$ in the Brauer group is 2). On the other hand, if D has trivial corestriction along K/k and D contains a k-subalgebra of dimension 4, then D would be the restriction of that algebra. Then applying $\mathrm{cor} \circ \mathrm{res}$ would yield the identity element of the Brauer group. This is impossible so we may conclude that

- if K/k is a separable cubic extension such that D has trivial corestriction along K/k, then D contains no k-subalgebra of dimension 4.

Let R be a division algebra of degree d having center F (with $D \neq F$, so that F is infinite). Let F/F_0 be a separable field extension of degree n. Let $\mathrm{tr}: F \to F_0$ be the trace map. Since F/F_0 is separable, tr is surjective. Let

$$b_1, \ldots, b_{n-1} \text{ be a basis for } S := \{a \in F\colon\ \mathrm{tr}(a) = 0\}.$$

Lemma 3.1. (Well known) *For any element $a \in F^{\times}$ we have: $a \in F_0$ iff $\mathrm{tr}(ab_k) = 0$, for all $1 \leqslant k \leqslant n-1$.*

Proof. We must show that $a \in F_0$ iff $aS \subseteq S$. For $a \in F_0$ obviously $aS \subseteq S$. Conversely suppose $aS \subseteq S$. Write $a = a_0 + a_1$ with $a_0 \in F_0$ and $a_1 \in S$. Since $a_0 S \subseteq S$, we get that $a_1 S \subseteq S$. But $a_1 F_0 \subseteq S$ so $a_1(F_0 + S) \subseteq S$, that is $a_1 F \subseteq S$, which is possible iff $a_1 = 0$. $\square$

For an element $a \in R$, we let

$$\alpha_0(a) + \alpha_1(a)x + \alpha_2(a)x^2 + \cdots + \alpha_d(a)x^d, \quad \alpha_d(a) = 1,$$

be the characteristic polynomial of a (over F). Let

$$V_0 = \{a \in R^\times \mid \mathfrak{N}(a) \in F_0\} \quad \text{and} \quad Z_0 = \{a \in R^\times \mid \alpha_i(a) \in F_0, \text{ for all } i\},$$

and note that V_0 is a subgroup of $R^\times$.

Lemma 3.2. *Let $\lambda_1, \lambda_2, \ldots, \lambda_{d+1} \in F_0$ be $d+1$ distinct elements. Suppose that $a_0, a_1, \ldots, a_d \in F$ are elements such that*

$$a_0\lambda_j^0 + a_1\lambda_j^1 + a_2\lambda_j^2 + \cdots + a_d\lambda_j^d \in F_0,$$

for all $1 \leqslant j \leqslant d+1$. Then $a_i \in F_0$, for all $0 \leqslant i \leqslant d$.

Proof. Let $b_1, \ldots, b_{n-1}$ be as above. We show that for each $0 \leqslant i \leqslant d$ and each $1 \leqslant k \leqslant n-1$, $\operatorname{tr}(a_i b_k) = 0$, then Lemma 3.1 completes the proof.

We use a Vandermonde argument. For each $1 \leqslant k \leqslant n-1$,

$$0 = \operatorname{tr}\left(\sum_{i=0}^{d} \lambda_j^i a_i b_k\right) = \sum_{i=0}^{d} \lambda_j^i \operatorname{tr}(a_i b_k).$$

Fixing k we have a homogeneous system of $d+1$ linear equations in $d+1$ variables with simultaneous solution the $\operatorname{tr}(a_i b_k)$, and the coefficient matrix (λ_j^i) has nonzero determinant, so the solution must be trivial, i.e. $\operatorname{tr}(a_i b_k) = 0$, for all i and k. $\square$

As a corollary we get,

Lemma 3.3. *If $V_0 \cup \{0\}$ contains a F_0-subspace W_0 then for each $0 \neq x \in W_0$, $x^{-1}W_0 \subseteq Z_0$.*

Proof. Let $x \in W_0$, with $x \neq 0$. Then $x^{-1}W_0 \subseteq V_0$ and $x^{-1}W_0$ is a F_0-subspace. Thus we assume that $1 \in W_0$ and we will prove that $W_0 \subseteq Z_0$.

Let $a \in W_0$. Then $\lambda - a \in W_0$ for each $\lambda \in F_0$, and thus

$$\sum_{i=0}^{d} \alpha_i(a)\lambda^i = \mathfrak{N}(\lambda - a) \in F_0, \tag{$*$}$$

because the minimal polynomial of $\lambda - a$ is $\sum_{i=0}^{d} \alpha_i(a)(\lambda - x)^i$ and thus putting $x = 0$ in the characteristic polynomial of $\lambda - a$ gives us the norm of $\lambda - a$. Now choose in Eq. $(*)$ distinct $\lambda = \lambda_j$, $j = 1, \ldots, d+1$, and use Lemma 3.2 (with $\alpha_i(a)$ in place of a_i). $\square$

Lemma 3.4. *Assume that* $\mathrm{char}(D) \neq 2$ *and let* V *and* U *be as in the introduction.*

(1) *If* $V \cup \{0\}$ *contains a* k*-subspace of dimension* 3*, then there exists a* k*-subalgebra of* D *of dimension* 4;
(2) *if the corestriction of* D *to* k *is trivial, then* $V \cup \{0\}$ *contains no* k*-subspace of dimension* 3.

Proof. (1) Suppose that $V \cup \{0\}$ contains a k-subspace of dimension 3. Then, by Lemma 3.3, there exists a k-subspace $W \subseteq U \cup \{0\}$ of dimension 3, with $1 \in W$. We show that there are pure elements $e, f \in W$ such that $ef = -fe$. Then the k-span of $1, e, f, ef$ is a k-subalgebra of dimension 4. Since the trace map takes W to k, $\dim_k(\mathrm{Pure}(W) \cup \{0\}) = 2$, where $\mathrm{Pure}(W) = W \cap \mathrm{Pure}(D)$. Let $e, g \in W \cap \mathrm{Pure}(D)$ be linearly independent. Then by Lemma 2.3, we can write $g = \alpha e + f$, where f is pure and anti-commutes with e and $\alpha \in K$. We claim that $\alpha \in k$, then also $f \in W$ and we are done. Now $k \ni \mathfrak{N}(e+g) = (e+g)(\bar{e}+\bar{g}) = \mathfrak{N}(e) + \mathfrak{N}(g) + \mathfrak{T}(e\bar{g})$. Since $\mathfrak{N}(e+g), \mathfrak{N}(e), \mathfrak{N}(g) \in k$, we see that $\mathfrak{T}(e\bar{g}) = \mathfrak{T}(-eg) \in k$, which implies that $\alpha \in k$.

(2) This follows from (1) and the fact that when the corestriction of D to k is trivial, D contains no k-subalgebra of dimension 4. $\square$

4. Some simple dimension considerations

In this section R is a finite-dimensional division algebra and F is its center. We recall the following lemma from [S, Lemma 1.1], which is used repeatedly in our proofs.

Lemma 4.1. *Let* $M \lhd R^\times$ *and let* $\bullet : R^\times \to R^\times/M$ *be the canonical homomorphism. Let* $x \in R^\times$ *and* $n \in M$*, with* $n \neq -x$*. Then* $[x^\bullet, (x+n)^\bullet] = 1^\bullet$.

Proof. We have $(x+n)^\bullet = (n(n^{-1}x+1))^\bullet = (n^{-1}x+1)^\bullet$. Since $n^{-1}x+1$ commutes with $n^{-1}x$ in $R^\times$, we see that $(n^{-1}x+1)^\bullet$ commutes with $(n^{-1}x)^\bullet = x^\bullet$ in $R^\times/M$. $\square$

Proposition 4.2. *Let* $F_0 \subseteq F$ *be a subfield, with* $[F : F_0] < \infty$.

(1) *If* $H \leqslant R^\times$ *is a subgroup, and* H *contains* $W \setminus \{0\}$*, for some* F_0*-subspace* W *of* R *of dimension* $> \frac{1}{2}\dim_{F_0} R$*, then* $H = R^\times$;
(2) *if* $M \lhd R^\times$ *is a normal subgroup and* M *contains* $W \setminus \{0\}$*, for some* F_0*-subspace* W *of* R *of dimension* $> \frac{1}{4}\dim_{F_0} R$*, then* $R^\times/M$ *is abelian*;
(3) *if* $d = \deg(R) = 2$ *or* 3 *and* $M \lhd R^\times$ *contains* $P^\times$*, for some maximal subfield* P *of* R*, then* $R^\times/M$ *is abelian* (*and hence an elementary abelian* d*-group*).

Proof. For a subset $X \subseteq R$, let $X^\times := X \setminus \{0\}$. Let $\bullet : R^\times \to R^\times/M$ be the canonical homomorphism.

(1) Choose a coset Hx of H in $R^\times$. Then $(Wx)^\times \subseteq Hx$ and our hypothesis on $\dim_{F_0} W$ implies that $W \cap Wx$ contains a nonzero element, so $H \cap Hx \neq \emptyset$, implying $H = Hx$ and it follows that $H = R^\times$.

(2) Let $x \in R^\times \setminus M$, then $M + Mx$ contains $(W + Wx)^\times$. Since $\dim_{F_0}(W + Wx) > \frac{1}{2}\dim_{F_0}(R)$, we get by (1) that $R^\times = \langle M + Mx\rangle$. Note now that by Lemma 4.1, for each $r \in M + Mx$, $r^\bullet$ commutes with $x^\bullet$. It follows that $x^\bullet$ is in the center of $R^\times/M$. As this holds for all $x \in R^\times \setminus M$, $R^\times/M$ is abelian.

(3) Take $F_0 = F$. Since $\dim_F(P) = 2$ (respectively 3), we see that $\dim_F(P) > \frac{1}{4}\dim_F(R)$, so by (2), $R^\times/M$ is abelian. Thus $M \geqslant [R^\times, R^\times]$. Since $x^d \in F^\times[R^\times, R^\times]$ (see, e.g., [RoS, Section 0]), we see that $R^\times/M$ is an elementary abelian d-group. □

5. Preliminaries on normal subgroups of $D^\times$

In this section $M \lhd D^\times$ such that $K^\times \leqslant M$. We let $*: D^\times \to D^\times/M$ be the canonical homomorphism. In the case when $\mathrm{char}(K) \neq 2$ we let

$$S := K^\times\big\langle 2w + 1 \mid w \in \mathrm{SL}_1(D)\big\rangle.$$

Notice that $S \lhd D^\times$. We let $\bullet: D^\times \to D^\times/S$ be the canonical homomorphism. We caution here that whenever we write $a^\bullet$ or a^* for $a \in D$ it is automatically assumed that $a \neq 0$.

Remark 5.1. The following observation will be used throughout this section with no further comment. Let $x \in D^\times$, $m \in M$ and $w \in \mathrm{SL}_1(D)$. Consider the element $(xw + m)^g$, $g \in D^\times$. If $m \in K^\times$, then $(xw + m)^g = x^g w^g + m = xx^{-1}x^g w^g + m = xv + m$, for some $v \in \mathrm{SL}_1(D)$. In general, $(xw + m)^g = (m(m^{-1}xw + 1))^g = m^g(m^{-1}xv + 1) = m^g m^{-1}(xv + m)$, for some $v \in \mathrm{SL}_1(D)$. Hence $\langle xw + m \mid w \in \mathrm{SL}_1(D)\rangle$ is a normal subgroup of $D^\times$ if $m \in K^\times$, and $M\langle xw + m \mid w \in \mathrm{SL}_1(D)\rangle$ is always a normal subgroup of $D^\times$.

Lemma 5.2. *Let $x \in D^\times$ and suppose $x = n + m$, with $m, n \in M$. Then*

$$\big[x^*, (xw + m)^*\big] = 1^*,$$

for all $w \in \mathrm{SL}_1(D)$.

Proof. Assume first that $m = 1$. Then $xw + m = (n + 1)w + 1 = (n + 1 + w^{-1})w$. By Lemma 2.7, $(1 + w^{-1})^2 = (\mathfrak{T}(w^{-1}) + 2)w^{-1} \in K^\times w^{-1}$, and by Lemma 4.1,

$$\big[\big(n + 1 + w^{-1}\big)^*, \big(1 + w^{-1}\big)^*\big] = 1^*,$$

it follows that $[(n + 1 + w^{-1})^*, (w^{-1})^*] = 1^*$. Consequently $[((n + 1)w + 1)^*, w^*] = 1^*$, and hence also $[((n + 1)w + 1)^*, (n + 1)^*] = 1^*$, i.e., $[x^*, (xw + 1)^*] = 1^*$.

Next, $m^{-1}x = m^{-1}n + 1$, so by the previous paragraph, for all $w \in \mathrm{SL}_1(D)$, $[(m^{-1}x)^*, (m^{-1}xw + 1)^*] = 1^*$, and the lemma follows. □

Lemma 5.3. *Let $y \in D^\times$ and $m \in M$ and suppose that $yw + m \in M$, for all $w \in \mathrm{SL}_1(D)$. Then,*

(1) $[(xyw+m)^*, (x^{-1}v+1)^*] = 1^*$, *for all* $x \in D^\times$ *and* $v, w \in \mathrm{SL}_1(D)$;
(2) *if for some* $x \in D^\times$, $\{xw+1 \mid w \in \mathrm{SL}_1(D)\} \subseteq M$, *then* $[(xyw+m)^*, x^*] = 1^* = [(xyw+m)^*, v^*]$, *for all* $v, w \in \mathrm{SL}_1(D)$; *in particular,*
(3) *if* $m = 1$, *then* $[(\mathfrak{N}(y)w+1)^*, y^*] = 1^* = [(\mathfrak{N}(y)w+1)^*, v^*]$, *for all* $v, w \in \mathrm{SL}_1(D)$.
(4) $[(y+n)^*, ((y+n)w+m)^*] = 1^*$, *for all* $n \in M \cup \{0\}$ *and* $w \in \mathrm{SL}_1(D)$; *in particular,*
(5) *if* $\mathrm{char}(D) \neq 2$ *and* $\{(e+\alpha)w+1 \mid w \in \mathrm{SL}_1(D)\} \subseteq M$, *for some* $e \in \mathrm{Pure}(D)$ *and* $\alpha \in K$, *then* $[(e+\gamma), (e+\gamma)w+1]^* = 1^*$, *for all* $\gamma \in K$ *and* $w \in \mathrm{SL}_1(D)$.

Proof. (1) Let $w \in \mathrm{SL}_1(D)$ and $x \in D^\times$. Then $xyw+m = x(yw+x^{-1}m) = x(yw-m+m+x^{-1}m)$. Now since $yw-m \in M$, it follows that $[(1+x^{-1})^*, (yw-m+m+x^{-1}m)^*] = 1^*$ (see Lemma 4.1), and hence also

$$\left[\left(1+x^{-1}\right)^*, (xyw+m)^*\right] = 1^*. \tag{$*$}$$

Now in $(*)$, replace x by $v^{-1}x$, $v \in \mathrm{SL}_1(D)$, to get $[(1+x^{-1}v)^*, (v^{-1}xyw+m)^*] = 1^*$, and note that $\{v^{-1}xyw+m \mid w \in \mathrm{SL}_1(D)\} = \{xyw+m \mid w \in \mathrm{SL}_1(D)\}$. This shows (1).

(2) By (1), $[(xyw+m)^*, ((xv)^{-1}+1)^*] = 1^*$ (notice that $(xv)^{-1} = x^{-1}u$, with $u = xv^{-1}x^{-1} \in \mathrm{SL}_1(D)$), for all $v, w \in \mathrm{SL}_1(D)$, and since $xv+1 \in M$, $((xv)^{-1}+1)^* = ((xv)^{-1})^*$, so

$$\left[(xyw+m)^*, (xv)^*\right] = 1^*, \quad \text{for all } v, w \in \mathrm{SL}_1(D).$$

This implies (2).

(3) Since, by hypothesis, $yw+1 \in M$, for all $w \in \mathrm{SL}_1(D)$, also $\bar{y}w+1 \in M$, for all $w \in \mathrm{SL}_1(D)$. Then, taking $\bar{y}$ in place of y and y in place of x in (2) we get (3).

(4) Let $w \in \mathrm{SL}_1(D)$. Since $yw+m \in M$, $(y+mw^{-1})^* = (w^{-1})^*$. Now

$$(y+n)w+m = \left(n+y+mw^{-1}\right)w.$$

By Lemma 4.1, $[(y+mw^{-1})^*, (n+y+mw^{-1})^*] = 1^*$, so $[(w^{-1})^*, (n+y+mw^{-1})^*] = 1^*$, and it follows that $[((y+n)w+m)^*, w^*] = 1^*$. Hence also $[(y+n)^*, ((y+n)w+m)^*] = 1^*$, and (4) is proved.

(5) follows from (4), just take $y = e+\alpha$, $m = 1$ and $n \in K$. $\square$

Lemma 5.4. *Let* $x, y \in D^\times$ *and* $m_1, m_2 \in M$ *and consider the following hypotheses*:

(i) $[x^*, (xw+m_1)^*] = 1^*$, *for all* $w \in \mathrm{SL}_1(D)$.
(ii) $yw+m_2 \in M$, *for all* $w \in \mathrm{SL}_1(D)$.

Then,

(1)(i) *implies that*

$$\left[\left\langle (x \pm n)^{D^\times}\right\rangle^*, (nw+m_1)^*, \left\langle x^{D^\times}\right\rangle^*\right] = 1^*,$$

for all $n \in M \cup \{0\}$ *and* $w \in \mathrm{SL}_1(D)$;

(2)(ii) *implies that*

$$\left[\left\langle (y+m\pm n)^{D^\times}\right\rangle^*, (nw+m_2)^*, \left\langle (y+m)^{D^\times}\right\rangle^*\right] = 1^*,$$

for all $m, n \in M \cup \{0\}$ *and* $w \in \mathrm{SL}_1(D)$.

Proof. (1) Fix $n \in M$ and let $T = M\langle xw + m_1 \mid w \in \mathrm{SL}_1(D)\rangle$. Let $\epsilon \in \{1, -1\}$ and $v \in \mathrm{SL}_1(D)$. Then $T \ni xv + m_1 = (x+\epsilon n)v - \epsilon nv + m_1$. Since $T \lhd D^\times$, Lemma 4.1 implies that, $[(x+\epsilon n)v, (-\epsilon nv + m_1)] \in T$. Also, by Lemma 4.1, $[v^*, (-\epsilon nv + m_1)^*] = 1^*$. It follows that $[(x+\epsilon n), (-\epsilon nv + m_1)] \in T$. As this holds for all $v \in \mathrm{SL}_1(D)$, we see that $[\langle (x+\epsilon n)^{D^\times}\rangle, \langle nw + m_1 \mid w \in \mathrm{SL}_1(D)\rangle] \leqslant T$. By hypothesis (i), $[T, x] \leqslant M$, so $[T, \langle x^{D^\times}\rangle] \leqslant M$, and (1) follows.

(2) Since $yw + m_2 \in M$, for all $w \in \mathrm{SL}_1(D)$, Lemma 5.3(4), implies that

$$\left[(y+m)^*, \left((y+m)w + m_2\right)^*\right] = 1^*,$$

for all $m \in M \cup \{0\}$ and $w \in \mathrm{SL}_1(D)$. Now apply (1) to $x = y + m$, to get (2). □

Lemma 5.5.

(1) $[\langle (n-\alpha)^{D^\times}\rangle, \langle (n+\alpha)^{D^\times}\rangle, S]^* = 1^*$, *for all* $n \in M$ *and* $\alpha \in K$;
(2) *suppose that* $\{yw + 1 \mid w \in \mathrm{SL}_1(D)\} \subseteq M$, *for some* $y \in D^\times$. *Then*

$$\left[\left\langle (y+\alpha)^{D^\times}\right\rangle, \left\langle (y+\beta)^{D^\times}\right\rangle, (\alpha-\beta)w + 1\right]^* = 1^*,$$

for all $\alpha, \beta \in K$, *and* $w \in \mathrm{SL}_1(D)$. *In particular,*
(3) *suppose* $\mathrm{char}(K) \neq 2$ *and that* $\{(e+\gamma)w + 1 \mid w \in \mathrm{SL}_1(D)\} \subseteq M$, *for some* $e \in \mathrm{Pure}(D)$ *and* $\gamma \in K$. *Then* $[\langle (e+\delta)^{D^\times}\rangle, \langle (e+\delta)^{D^\times}\rangle, 2\delta w + 1]^* = 1^*$, *for all* $\delta \in K^\times$ *and* $w \in \mathrm{SL}_1(D)$;
(4) *if* $\mathrm{char}(K) \neq 2$, *then*

$$\left[\left(e+\frac{1}{2}\right)^{D^\times}, \left(e+\frac{1}{2}\right)^{D^\times}\right] \leqslant K^\times\left\langle (e+\alpha)w + 1 \mid w \in \mathrm{SL}_1(D)\right\rangle,$$

for all $e \in \mathrm{Pure}(D)$ *and* $\alpha \in K$.

Proof. (1) Let $x = n - \alpha$ and $y = n + \alpha$. By Lemma 5.2, $[x^*, (xw+\alpha)^*] = 1^* = [y^*, (yw+\alpha)^*]$. By Lemma 5.4(1) (taking 2α in place of n and α in place of m_1), $[\langle (x+2\alpha)^{D^\times}\rangle^*, (2\alpha w+\alpha)^*, \langle x^{D^\times}\rangle^*] = 1^*$, for all $w \in \mathrm{SL}_1(D)$, that is, $[\langle y^{D^\times}\rangle^*, (2w+1)^*, \langle x^{D^\times}\rangle^*] = 1^*$, for all $w \in \mathrm{SL}_1(D)$. Next take y in place of x, 2α in place of n and α in place of m_1, in Lemma 5.4(1), to get $[\langle (y-2\alpha)^{D^\times}\rangle^*, (2\alpha w+\alpha)^*, \langle y^{D^\times}\rangle^*] = 1^*$, for all $w \in \mathrm{SL}_1(D)$, or $[\langle x^{D^\times}\rangle^*, (2w+1)^*, \langle y^{D^\times}\rangle^*] = 1^*$, for all $w \in \mathrm{SL}_1(D)$. By the three subgroup lemma (see [A]) $[\langle x^{D^\times}\rangle, \langle y^{D^\times}\rangle, S]^* = 1^*$.

(2) By Lemma 5.4(2), $[\langle (y+\beta+(\alpha-\beta))^{D^\times}\rangle, \langle (\alpha-\beta)w+1, (y+\beta)^{D^\times}\rangle]^* = 1^*$, and $[\langle (y+\alpha+(\beta-\alpha))^{D^\times}\rangle, (\alpha-\beta)w+1, \langle (y+\alpha)^{D^\times}\rangle]^* = 1^*$, for all $w \in \mathrm{SL}_1(D)$. Again the three subgroup lemma completes the proof of (2).

(3) Take in (2), $y = e+\gamma$, $\alpha = \delta-\gamma$ and $\beta = -\delta-\gamma$. Then $\alpha-\beta = 2\delta$, $y+\alpha = e+\delta$ and $y+\beta = e-\delta$, so (3) follows from (2).

(4) Let $\alpha \in K$ and assume $M = K^\times\langle (e+\alpha)w+1 \mid w \in \mathrm{SL}_1(D)\rangle$. By Lemma 5.3(5), $[e+\gamma, (e+\gamma)w+1]^* = 1^*$, for all $\gamma \in K$ and $w \in \mathrm{SL}_1(D)$. Note that this implies that $[\langle (e+\gamma)^{D^\times}\rangle, \langle (-e-\gamma+1)^{D^\times}\rangle]^* = 1^*$, for all $\gamma \in K$. This is because the subgroup $H := \langle (e+\gamma)w+1 \mid w \in \mathrm{SL}_1(D)\rangle$ is normal $D^\times$ (see Remark 5.1), so $\langle (e+\gamma)^{D^\times}\rangle$ commutes with it, and $-e-\gamma+1 \in H$. Now, taking $\gamma = \frac{1}{2}$ we get $[\langle (e+\frac{1}{2})^{D^\times}\rangle, \langle (-e+\frac{1}{2})^{D^\times}\rangle]^* = 1^*$ and (4) follows. □

Lemma 5.6. *Assume that* $\mathrm{char}(K) \neq 2$*, then*

(1) *for each* $x \in D^\times$ *and* $v, w \in \mathrm{SL}_1(D)$*,* $[(2xw+1)^\bullet, (x^{-1}v+1)^\bullet] = 1^\bullet$*;*
(2) *for each* $-1 \neq x \in D^\times$ *and* $v, w \in \mathrm{SL}_1(D)$*,* $[((1+x)w+1)^\bullet, ((\frac{1-x}{1+x}+1)v+1)^\bullet] = 1^\bullet$*;*
(3) *for* $e \in \mathrm{Pure}(D)$*,* $[\langle e^{D^\times}\rangle^\bullet, \mathrm{SL}_1(K(e))^\bullet] = 1$*, in particular,*

$$\left[\left\langle \mathrm{SL}_1\left(K(e)\right)^{D^\times}\right\rangle^\bullet, \left\langle \mathrm{SL}_1\left(K(f)\right)^{D^\times}\right\rangle^\bullet\right] = 1^\bullet,$$

for all $f \in \mathrm{Pure}(D)$ *that anti-commutes with* e*.*

Proof. Take $y = 2$ and $m = 1$ in Lemma 5.3(1) (take S in place of M there) to get (1). For (2) replace x^{-1} by $1+x$ in (1) to get $[((1+x)v+1)^\bullet, (\frac{2}{1+x}w+1)^\bullet] = 1^\bullet$, and note that $\frac{2}{1+x} = \frac{1-x}{1+x}+1$. Finally, for (3), take in (2), $x = e$, to get $[(((1+e)w+1)^\bullet, (\frac{1-e}{1+e}+1)v+1)^\bullet] = 1^\bullet$. Taking $w = -1$ and $v = -1$, we get $[\langle e^{D^\times}\rangle^\bullet, \langle (\frac{1-e}{1+e})^{D^\times}\rangle^\bullet] = 1^\bullet$. Now replace e by αe, $\alpha \in K^\times$, and use Lemma 2.6, to get the first part of (3). The second part of (3) follows from Lemma 2.10. □

Lemma 5.7. *Assume that* $\mathrm{char}(K) \neq 2$*, then*

(1) *let* $S_1 = S$ *and* $S_{k+1} = \langle S_k, \{2^{k+1}w+1 \mid w \in \mathrm{SL}_1(D)\}\rangle$*,* $k \geqslant 1$*. Then for each* $k \geqslant 2$*, we have*

$$\left[K^\times\left\langle \left(2^k w+1\right) \mid w \in \mathrm{SL}_1(D)\right\rangle,\ \mathrm{SL}_1(D)\right] \leqslant S_{k-1};$$

(2) *if* $\mathrm{char}(K) > 2$*, and* t *is the first positive integer such that* $2^t = 1$ *in* K*, then* $\mathrm{SL}_1(D)^\bullet$ *is nilpotent of class* $\leqslant t-1$*.*

Proof. (1) Since $2^{k-1}w+1, 2w+1 \in S_{k-1}$, for all $w \in \mathrm{SL}_1(D)$, Lemma 5.3(2) (with S_{k-1} in place of M, $y = 2$, $x = 2^{k-1}$ and $m = 1$) implies that $[(2^k w+1), \mathrm{SL}_1(D)] \leqslant S_{k-1}$, which is (1).

(2) Let $T_i = S_i \cap \mathrm{SL}_1(D)$. By (1), $[T_i, \mathrm{SL}_1(D)] \leqslant T_{i-1}$, for all $i \geqslant 2$. By Lemma 2.12, $S_t = D^\times$, so $T_t = \mathrm{SL}_1(D)$ and (2) follows from (1). □

Lemma 5.8. *Assume that* $\mathrm{char}(K) \neq 2$*, let* $e \in \mathrm{Pure}(D)$ *and set* $u := \frac{1-e}{1+e}$*. Then,*

(1) $e = \frac{1-u}{1+u}$;
(2) $2 - e = \frac{1+3u}{1+u}$, *and* $2 + e = \frac{3+u}{1+u}$.

In particular if $T = K^\times\langle 1 + 3w \mid w \in \mathrm{SL}_1(D)\rangle$*, then* $(1+e)^\star = (2-e)^\star$*, where* $\star : D^\times \to D^\times/T$ *is the canonical homomorphism.*

Proof. $1 - u = 1 - \frac{1-e}{1+e} = \frac{(1+e)-(1-e)}{1+e} = \frac{2e}{1+e}$. Similarly $1 + u = \frac{2}{1+e}$. So (1) holds. By (1), $2 - e = 2 - \frac{1-u}{1+u} = \frac{2(1+u)-(1-u)}{1+u} = \frac{1+3u}{1+u}$ and $2 + e = 2 + \frac{1-u}{1+u} = \frac{2(1+u)+(1-u)}{1+u} = \frac{3+u}{1+u}$, so (2) holds. Now, by (2), $(2-e)^\star = (\frac{1+3u}{1+u})^\star = (\frac{1}{1+u})^\star$. Since $1 + u = \frac{2}{1+e}$, $(\frac{1}{1+u})^\star = (1+e)^\star$. □

Proposition 5.9. *Let* $\mathrm{char}(K) \neq 2$*, pick* $e \in \mathrm{Pure}(D)$ *and assume that for all* $\alpha \in K^\times$*,* $\langle (1+\alpha e)^{D^\times}\rangle^*$ *is abelian. Then* $\mathrm{SL}_1(D)^*$ *is a* 2*-Engel group. In particular* $\mathrm{SL}_1(D)^*$ *is nilpotent of class* $\leqslant 3$.

Proof. For each $\alpha \in K^\times$, let $X_\alpha := K^\times\langle (1+\alpha e)^{D^\times}\rangle$. Our hypothesis implies that X_α^* is abelian, for all $\alpha \in K^\times$. By Lemma 2.11, for each $u \in \mathrm{SL}_1(D)$, there exists $x \in K(e)$ and $g \in D^\times$ such that $u = [x, g]$. But $x \in X_\alpha$, for some $\alpha \in K^\times$, so $u = [x, g] \in X_\alpha$. Hence for each $u \in \mathrm{SL}_1(D)$, there exists $\alpha \in K^\times$ such that $u \in X_\alpha$. Thus $\langle u^{D^\times}\rangle^*$ is abelian. It follows from Theorem 2.9 that $\mathrm{SL}_1(D)^*$ is nilpotent of class $\leqslant 3$. □

6. Normal subgroups containing a pure quaternion

Throughout this section *we assume that* $\mathrm{char}(K) \neq 2$. We let $K^\times \leqslant N \lhd D^\times$ containing a pure quaternion $e \in N \cap \mathrm{Pure}(D)$; we let $* : D^\times \to D^\times/N$ be the canonical homomorphism and we set $S = K^\times\langle 2w + 1 \mid w \in \mathrm{SL}_1(D)\rangle$. For $\alpha \in K^\times$, we let

$$X_\alpha := K^\times\big\langle (1+\alpha e)^{D^\times}\big\rangle \quad \text{and} \quad M := K^\times\big\langle [X_\alpha, X_\alpha] \mid \alpha \in K^\times\big\rangle.$$

Before we state the main theorem of this section we note that

$$(M \cap S)N \leqslant MN \leqslant K^\times \mathrm{SL}_1(D)N = \mathrm{SL}_1(D)N.$$

In this section we prove

Theorem 6.1.

(1) $[M, S]^* = 1$.
(2) *If* $\mathrm{char}(K) > 2$ *and* t *is the first positive integer such that* $2^t = 1$ *in* K*, then in the normal series*

$$N \lhd (M \cap S)N \lhd \mathrm{SL}_1(D)N \lhd D^\times,$$

$(M \cap S)N/N$ is abelian, $\mathrm{SL}_1(D)N/(M \cap S)N$ *is nilpotent of class* $\leqslant \max\{3, t-1\}$ *and* $D^\times/\mathrm{SL}_1(D)N$ *is abelian.*

We need the following lemma.

Lemma 6.2.

(1) $[X_\beta, X_\beta, S] \leqslant N$, *for each* $\beta \in K^\times$.
(2) $[M, S] \leqslant N$.
(3) $\mathrm{SL}_1(D)M/M$ *is nilpotent of class* $\leqslant 3$.

Proof. For (1), take $n = \beta e$ and $\alpha = 1$ in Lemma 5.5(1) and note that $K^\times\langle(\beta e + 1)^{D^\times}\rangle = X_\beta = K^\times\langle(\beta e - 1)^{D^\times}\rangle$. Part (2) follows from (1). For part (3) use Proposition 5.9, and notice that M satisfies the hypothesis of that proposition. $\square$

Proof of Theorem 6.1. Part (1) of the theorem is Lemma 6.2(2). Now by Lemma 5.7, $\mathrm{SL}_1(D)S/S$ is nilpotent of class $\leqslant t-1$ and by Lemma 6.2(3), $\mathrm{SL}_1(D)M/M$ is nilpotent of class $\leqslant 3$. Thus for $c = \max\{3, t-1\}$, $\Gamma_c(\mathrm{SL}_1(D)) \leqslant M \cap S$. Of course since $[M, S]^* = 1^*$, $(M \cap S)N/N$ is abelian. This completes the proof of Theorem 6.1. $\square$

We conclude with a result which holds both in characteristic zero and in positive odd characteristic.

Lemma 6.3. *If* $\{1 + 3w \mid w \in \mathrm{SL}_1(D)\} \subseteq N$, *then* $\mathrm{SL}_1(D)^*$ *is nilpotent of class* $\leqslant 3$.

Proof. Suppose $\{1 + 3w \mid w \in \mathrm{SL}_1(D)\} \subseteq N$. We show $\langle(1 + \alpha e)^{D^\times}\rangle^*$ is abelian, for all $\alpha \in K^\times$, then Proposition 5.9 completes the proof. By Lemma 5.2 (with αe in place of n and 1 in place of m; see also Remark 5.1), $[\langle(\alpha e + 1)^{D^\times}\rangle^*, \langle(\alpha e + 2)^{D^\times}\rangle^*] = 1^*$. But $(1 + \alpha e)^* = (2 - \alpha e)^*$ (by the final statement in Lemma 5.8 taking αe in place of e) implying that $\langle(1 + \alpha e)^{D^\times}\rangle^*$ is abelian (because $(2 - \alpha e)^* = (\frac{1}{2+\alpha e})^*$). $\square$

Corollary 6.4. *Let D be a quaternion division algebra of characteristic* 3, *and let* $e \in D \setminus K$ *be an element such that* $e^2 \in K$. *Let N be the normal subgroup of* $D^\times$ *generated by e and* $K^\times$. *Then* $\mathrm{SL}_1(D)N/N$ *is nilpotent of class* $\leqslant 3$.

Proof. This follows from Lemma 6.3 since the condition $\{1 + 3w \mid w \in \mathrm{SL}_1(D)\} \subseteq N$ is automatically satisfied. $\square$

Acknowledgment

We thank the referee for a very careful reading of the paper and for very useful remarks.

References

[A] M. Aschbacher, Finite Group Theory, Cambridge Stud. Adv. Math., vol. 10, Cambridge Univ. Press, Cambridge, 2000.

[KMRT] M.-A. Knus, A.S. Merkurev, M. Rost, J.-P. Tignol, The Book of Involutions, Amer. Math. Soc. Colloq. Publ., vol. 44, Amer. Math. Soc., Providence, RI, 1998.

[L] F.W. Levi, Groups in which the commutator operation satisfies certain algebraic conditions, J. Indian Math. Soc. (N.S.) 6 (1942) 87–97.

[PRa] V.P. Platonov, A.S. Rapinchuk, On the group of rational points of three-dimensional groups, Soviet Math. Dokl. 20 (1979) 693–697.

[Pr] G. Prasad, The Kneser–Tits problem for triality forms, preprint, 2005.

[RaPo] A.S. Rapinchuk, A. Potapchik, Normal subgroups of $SL_{1,D}$ and the classification of finite simple groups, Proc. Indian Acad. Sci. 106 (1996) 329–368.

[RaRoS] A.S. Rapinchuk, L. Rowen, Y. Segev, Nonabelian free subgroups in homomorphic images of valued quaternion division algebras, Proc. Amer. Math. Soc., in press.

[RaS] A.S. Rapinchuk, Y. Segev, Valuation-like maps and the congruence subgroup property, Invent. Math. 144 (3) (2001) 571–607.

[RaSSei] A.S. Rapinchuk, Y. Segev, G.M. Seitz, Finite quotients of the multiplicative group of a finite-dimensional division algebra are solvable, J. Amer. Math. Soc. 15 (4) (2002) 929–978.

[Rob] D.J.S. Robinson, A Course in Group Theory, Grad. Texts in Math., vol. 80, Springer-Verlag, New York, 1996.

[RoS] L. Rowen, Y. Segev, The multiplicative group of a division algebra of degree 5 and Wedderburn's factorization theorem, in: Contemp. Math., vol. 259, 2000, pp. 475–486.

[S] Y. Segev, On finite homomorphic images of the multiplicative group of a division algebra, Ann. of Math. (2) 149 (1999) 219–251.

[Ti] J. Tits, Groupes de Whitehead de groupes algébriques simples sur un corps, d'aprés V.P. Platonov et al., Séminaire Bourbaki, 29e année, Exp. No. 505, 1976/7, pp. 218–236.